AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions of claims in the application:

Listing of Claims:

1-11. (Cancelled).

12. (Withdrawn) A secure automation device communication system comprising:

a certification component; and

a plurality of automation devices that interact with the certification component to generate and receive certificates which bind public keys to specific automation devices to facilitate identification of the devices that generate encrypted messages.

13. (Withdrawn) The system of claim 12, wherein the automation devices include programmable logic controllers, I/O devices, and communication adapters.

14. (Withdrawn) The system of claim 12, wherein the automation devices communicate messages over a local area network.

15. (Withdrawn) The system of claim 12, wherein certificates contain an automation device or user name or ID and a public key associated therewith.

16. (Withdrawn) The system of claim 12, wherein the certification component stores certificates in a certificate data store isolated from automation devices.

17. (Withdrawn) The system of claim 12, wherein automation devices contain private keys to facilitate encryption and/or decryption of messages.

18. (Withdrawn) The system of claim 12, wherein a first automation device utilizes one key in a public private key pair to create a secure message component that is transmitted to a second automation device.

19. (Withdrawn) The system of claim 18, wherein the second automation device receives the secure message component and utilizes the other key in a public private key pair to decrypt the message component.

20. (Withdrawn) The system of claim 12, wherein messages are digitally signed and include a message, message digest, and information regarding a hash algorithm.

21. (Withdrawn) The system of claim 20, wherein the hash algorithm is MD5.

22. (Withdrawn) A method of managing digital rights comprising:
defining rules of use concerning automation device program privileges;
downloading the rules to an automation device;
limiting interaction with the automation device based on the rules and an identity of a user.

23. (Withdrawn) The method of claim 22, wherein user identity is established via digital certificates.

24. (Withdrawn) The method of claim 23, wherein user digital certificates are generated by a local area control component.

25. (Withdrawn) The method of claim 23, wherein the user identity is established utilizing a SIM card.

26. (Withdrawn) The method of claim 23, wherein user identity is established employing biometrics.

27. (Withdrawn) The method of claim 22, wherein user rules prohibit particular users from viewing portions of an automation device program.

28. (Withdrawn) The method of claim 22, wherein user rules prohibit particular users from modifying a ladder logic program.

29. (Withdrawn) A computer readable medium having stored thereon computer executable instructions for carrying out the method of claim 22.

30-41. (Cancelled).

42. (New) A digital rights management system for use in an industrial environment comprising:

a processor;

a computer-readable storage medium operationally coupled to the processor and storing computer executable instructions, the computer executable instructions, when executed by the processor, implement components comprising:

a certification component that generates certificates for a specific automation device, the automation device controls an industrial process; and

an access component that establishes rules of use for the automation device based on at least one of the identification of an entity wanting to access the automation device.

43. (New) The system of claim 42, wherein the system is executed by a computer remotely located from the automation device.

44. (New) The system of claim 43, wherein communication between the automation device and the certification and access components is over a local area network.

45. (New) The system of claim 44, wherein communication is secured via digital certificates which bind public keys to specific users and/or entities to facilitate decryption of a message as well as identification of a sender.

46. (New) The system of claim 45, wherein the message is digitally signed to enable the message to be authenticated.

47. (New) The system of claim 42, wherein access to the access component is a restricted component limited to a particular user or group of users via certificates.

48. (New) The system of claim 42, wherein the automation device includes an access credential component that defines and restricts access to particular objects and services based on the identity of the user as established by a certificate.

49. (New) The system of claim 48, wherein the automation device includes a virtual key component adapted to retrieve identifying information from a certificate.

50. (New) The system of claim 48, wherein the access credential component also defines and restricts access based on a personal id provided by a SIM card.

51. (New) The system of claim 50, wherein the automation device includes a physical key component adapted to retrieve identifying information from the SIM card.

52. (New) The system of claim 42, wherein the automation device is one of a programmable logic controller, an I/O device, and a communication adaptor.

53. (New) An industrial automation device communication methodology comprising:

employing a processor executing computer executable instructions on a computer readable storage medium of a first automation device to implement the following acts:

encrypting, via the processor, a message to be sent to a second automation device utilizing a key derived from a certification component, the key has been uniquely created for the first automation device, where the first and second automation devices are associated with an industrial process; and

transmitting the encrypted message to the second automation device, wherein the certification component verifies identity of the first automation device of the message, and an access component establishes rules of use for the message based at least upon the identity of the automation device.

54. (New) The methodology of claim 53, further comprising:

receiving an encrypted message from a first automation device or device controller;

locating a certificate component associated with the first automation device sending the message; and

decrypting the message utilizing the public key provided by the certificate component.

55. (New) The method of claim 54, wherein at least one of the first or second automation devices is an industrial programmable logic controller (PLC).

56. (New) The method of claim 55, wherein the message is a PLC program.

57. (New) The method of claim 54, wherein locating the certificate component comprises searching a local automation device store.

58. (New) The method of claim 54, wherein locating the certificate comprises downloading the certificate from the certification component.

59. (New) A computer readable medium having stored thereon computer executable instructions for carrying out the method of claim 53.

60. (New) A method of industrial automation device communication comprising:

employing a processor executing computer executable instructions on a computer readable storage medium of a first automation device to implement the following acts:

associating a first industrial control device with a second industrial control device, the first and second control devices are associated with an industrial process;

generating, via the processor, a digitally signed message component comprising information uniquely associated with the first industrial control device or the second industrial control device including a message, a message digest, a certificate component, and hash function data, wherein the message component is generated by the first industrial automation device; and

transmitting the message component to the second industrial automation device, wherein a certification component verifies identity of at least one of the first or second automation devices, and an access component establishes rules of use for the message based upon the identity of at least one of the automation devices.

61. (New) The method of claim 60, further comprising encrypting the message component prior to transmission.

62. (New) The method of claim 61, further comprising receiving and decrypting the message component.

63. (New) The method of claim 60, further comprising authenticating the message by retrieving a hash function in accordance with the hash information, generating a message digest by applying the retrieved hash function to the received message and comparing the generated message digest with the message digest retrieved from the message component.

64. (New) A computer readable medium having stored thereon computer executable instructions for carrying out the method of claim 60.